IC CARD ISSUING SYSTEM, IC CARD PROCESSING SYSTEM, AND IC CARD

Veröffentlichungsnr. (Sek.)	JP2000172490
Veröffentlichungsdatum :	2000-06-23
Erfinder :	YAMADA HIROYOSHI
Anmelder :	TOSHIBA CORP
Veröffentlichungsnummer :	JP2000172490
Aktenzeichen: (EPIDOS-INPADOC-normiert)	JP19980341843 19981201
Prioritätsaktenzeichen: (EPIDOS-INPADOC-normiert)	
Klassifikationssymbol (IPC) :	G06F9/06; G06K17/00
Klassifikationssymbol (EC) :	
Korrespondierende Patentschriften	

Bibliographische Daten

PROBLEM TO BE SOLVED: To expand and determine a specific area of a nonvolatile memory by allowing the IC card to divide an application recording area of its nonvolatile memory by physical addresses according to an indication from an issuing device.

SOLUTION: While a terminal device 11 specifies an issuer, the issue, card ID, slot size, etc., of the card are indicated and an IC card 12 which is not recorded is inserted into the card insertion slot 120 of a reader writer 112. The slot size is set according to an application made by a person who installs an application. Consequently, the card ID set by the terminal device 11 is recorded in a system data area 31 of the nonvolatile memory(EEPROM) 23 and the addresses and sizes in user application areas 35 by slots are recorded in a slot management table 34a in the card data area 34 of the EEPROM 23, so that a symbol indicating the state of the corresponding application is recorded.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－172490
（P2000－172490A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
G06F 9/06	410	G06F 9/06	410B	5B058
	550		550Z	5B076
G06K 17/00		G06K 17/00	B	

審査請求　未請求　請求項の数８　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－341843

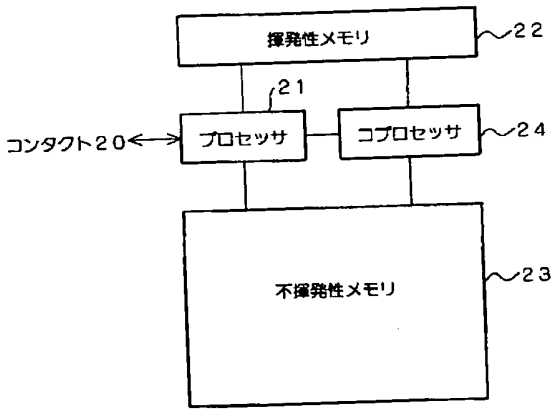
(22)出願日　平成10年12月１日(1998.12.1)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　山田　広佳
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B058 CA13 CA25 KA11
5B076 AA02 AA17 AB02 AB10 FC07

(54)【発明の名称】　ＩＣカード発行システムとＩＣカード処理システムとＩＣカード

(57)【要約】
【課題】　この発明は、アプリケーションが使用する領域をそのまま制限された物理領域にマッピングすることにより、領域管理をセキュリテイ管理と連動させ、アプリケーションの独立性を領域監視により確保することができる。
【解決手段】　この発明は、発行後にアプリケーションのインストールが可能なＩＣカードと、ＩＣカードへの入出力手段となる端末装置を具備するＩＣカードシステムにおいて、各アプリケーションが事前に確定されたスロット内でのみ領域を拡張しうるようにスロット領域を確定するようにしたものである。



【特許請求の範囲】
【請求項１】　不揮発性メモリを有するＩＣカードと、このＩＣカードを発行する発行装置とからなり、このＩＣカードの発行後に、このＩＣカードの不揮発性メモリにアプリケーションのインストールが行えるＩＣカード発行システムにおいて、
上記発行装置が、
アプリケーションをインストールする領域確保の指示を行う指示手段を有し、上記ＩＣカードが、
上記発行装置からのアプリケーション単位の領域確保の指示に基づいて、上記不揮発性メモリのアプリケーション記録領域を物理アドレスにより分割する分割手段を有することを特徴とするＩＣカード発行システム。
【請求項２】　不揮発性メモリを有するＩＣカードと、このＩＣカードにアプリケーションをインストールする処理装置とからなるＩＣカード処理システムにおいて、
上記処理装置が、
上記ＩＣカードの所定のスロットへのアプリケーションのインストールを指示する指示手段と、
この指示手段により指示されたアプリケーションを出力する出力手段とからなり、
上記ＩＣカードが、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、
この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなることを特徴とするＩＣカード処理システム。
【請求項３】　アプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションを処理する処理装置とからなるＩＣカード処理システムにおいて、
上記処理装置が、
上記ＩＣカードの所定のスロットのアプリケーションによる処理を指示する指示手段からなり、
上記ＩＣカードが、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、
この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、
この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とするＩＣカード処理システム。
【請求項４】　複数のモジュールからなるアプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションを処理する処理装置とからなるＩＣカード処理システムにおいて、
上記処理装置が、
上記ＩＣカードの所定のスロットのアプリケーションによる処理を指示する指示手段からなり、
上記ＩＣカードが、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する第１の記憶手段と、
上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、
この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記第１の記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する第１の判断手段と、
上記アプリケーション記録領域に記録されているアプリケーションのモジュールの利用を許可するアプリケーションを記憶する第２の記憶手段と、
上記第１の判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションのモジュールを利用すると判断した際に、上記第２の記憶手段に記憶されている許可条件に基づいて、そのモジュールの利用を許可するか否かを判断する第２の判断手段と、
この第２の判断手段により上記モジュールの利用を許可すると判断した際に、そのモジュールの処理を上記実行手段により実行し、上記第２の判断手段により上記モジュールの利用を許可しないと判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とするＩＣカード処理システム。
【請求項５】　アプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションの処理を指示する処理装置とからなるＩＣカード処理システムにおいて、
上記ＩＣカードが、

上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置から指示された所定のアプリケーション記録領域に記録されているアプリケーションの処理を実行する際、または所定のアプリケーションをスロット内にインストールする際に、他のスロットへアクセスするアプリケーションであるか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、
この判断手段によりアプリケーションのインストールまたは実行を不許可とする手段とからなることを特徴とするＩＣカード処理システム。
【請求項６】　アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するＩＣカードにおいて、
上記ＩＣカードは、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションのスロットを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、
この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなることを特徴とするＩＣカード。
【請求項７】　アプリケーションがインストールされている不揮発性メモリを有し、処理装置からの指示によりインストールされているアプリケーションを実行するＩＣカードにおいて、
上記ＩＣカードは、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、
この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、
この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とするＩＣカード。
【請求項８】　アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するＩＣカードにおいて、
上記ＩＣカードは、
上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、スロットを超過してアプリケーションが書込まれることを不許可とする手段を有することを特徴とするＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ＩＣカードの発行後に、このＩＣカードに対するアプリケーションのインストールが行えるＩＣカード発行システムとＩＣカード処理システムとＩＣカードに関する。
【０００２】
【従来の技術】従来のＩＣカードは、マスクＲＯＭにアプリケーションを予め書込み、書き換え可能な不揮発性メモリＥＥＰＲＯＭをデータ領域として使用している。
【０００３】このようなＩＣカードでは、アプリケーションを変更したり追加しようとした際に、新たにマスクＲＯＭを作り直したカードを発行（製造）しなければならず、開発期間や費用が掛かってしまうと言う問題がある。
【０００４】そこで、ＩＣカードの発行後に、このＩＣカードに対するアプリケーションのインストールが行え、追加、削除、更新が行えるＩＣカード処理システムが提案されている。このＩＣカードでは、複数のアプリケーションが扱えるようになっている。
【０００５】このシステムで用いられるＩＣカードでは、各アプリケーションごとにアプリケーションのＩＤが定義されているものの、物理的なアドレスは管理されていなかった。
【０００６】たとえば、図９に示すように、アプリケーションは、一般に複数の依存関係のあるソフトウェアモジュール（プログラムにおけるサブルーチンに対応）により構成される。図９の例では、３つのアプリケーション１、２、３が存在し、例えば、アプリケーション２はソフトウェアモジュール３２１、３２２、３２３、３２４により構成される。まず、アプリケーション２の入口として、ソフトウェアモジュール３２１を呼び出すことにより、要求に対する処理が開始される。ソフトウェアモジュール３２１は、その処理の中でソフトウェアモジュール３２２と３２３に部分的な処理を依頼する。ソフトウェアモジュール３２２は自身の処理を行い、その完了を依頼元であるソフトウェアモジュール３２１に通知する。また、ソフトウェアモジュール３２３は、さらにその部分的な処理をソフトウェアモジュール３２４に依頼し、その結果と自身の処理とを合わせて、依頼元であるソフトウェアモジュール３２１に通知する。ソフトウ

ェアモジュール３２１は全ての結果を回収し、自身の処理とを合わせて、アプリケーション２の全体としての結果を要求元に通知することになる。

【０００７】他のアプリケーション、ソフトウェアモジュールも同様に作用する。

【０００８】ここにおいて、アプリケーション１、２、３はソフトウェアモジュールの総体、として位置づけられる。また、上述の流れのなかで問題になるのは、ソフトウェアモジュール３２２と３１４の間に点線で示したようなアプリケーションを跨っての依存関係が定義される場合である。各アプリケーションは、異なる思想により、異なる設計者、異なる利益追求のために設計されていることが考えられ、不用意な他アプリケーションからの参照を許すと秘密漏洩、情報破壊などのセキュリテイ弱化を引き起こしかねないと言う問題がある。

【０００９】したがって、ＩＣカードの発行後に、このＩＣカードに対するアプリケーションのインストールが行えるＩＣカード処理システムにおいて、上記ＩＣカードが不揮発性メモリを有し、上記ＩＣカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域内でのみ領域を拡張しうるようにスロット領域を確定することができるものが要望されている。

【００１０】

【発明が解決しようとする課題】この発明は、ＩＣカードの発行後に、このＩＣカードに対するアプリケーションのインストールが行えるものにおいて、上記ＩＣカードが不揮発性メモリを有し、上記ＩＣカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域としてのスロット内でのみ領域を拡張しうるようにスロット領域を確定することができるＩＣカード発行システムとＩＣカード処理システムとＩＣカードを提供することを目的としている。

【００１１】

【課題を解決するための手段】この発明のＩＣカード発行システムは、不揮発性メモリを有するＩＣカードと、このＩＣカードを発行する発行装置とからなり、このＩＣカードの発行後に、このＩＣカードの不揮発性メモリにアプリケーションのインストールが行えるものにおいて、上記発行装置が、アプリケーションをインストールする領域確保の指示を行う指示手段を有し、上記ＩＣカードが、上記発行装置からのアプリケーション単位の領域確保の指示に基づいて、上記不揮発性メモリのアプリケーション記録領域を物理アドレスにより分割する分割手段を有するものである。

【００１２】この発明のＩＣカード処理システムは、不揮発性メモリを有するＩＣカードと、このＩＣカードにアプリケーションをインストールする処理装置とからなるものにおいて、上記処理装置が、上記ＩＣカードの所定のスロットへのアプリケーションのインストールを指示する指示手段と、この指示手段により指示されたアプリケーションを出力する出力手段とからなり、上記ＩＣカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなる。

【００１３】この発明のＩＣカード処理システムは、アプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションを処理する処理装置とからなるものにおいて、上記処理装置が、上記ＩＣカードの所定のスロットのアプリケーションによる処理を指示する指示手段からなり、上記ＩＣカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなる。

【００１４】この発明のＩＣカード処理システムは、複数のモジュールからなるアプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションを処理する処理装置とからなるものにおいて、上記処理装置が、上記ＩＣカードの所定のスロットのアプリケーションによる処理を指示する指示手段からなり、上記ＩＣカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する第１の記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記第１の記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する第１の判断手段と、上記アプリケーション記録領域に記録されているアプリケーションのモジュールの利用を許可す

るアプリケーションを記憶する第２の記憶手段と、上記第１の判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションのモジュールを利用すると判断した際に、上記第２の記憶手段に記憶されている許可条件に基づいて、そのモジュールの利用を許可するか否かを判断する第２の判断手段と、この第２の判断手段により上記モジュールの利用を許可すると判断した際に、そのモジュールの処理を上記実行手段により実行し、上記第２の判断手段により上記モジュールの利用を許可しないと判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする処理手段とからなる。

【００１５】この発明のＩＣカード処理システムは、アプリケーションがインストールされている不揮発性メモリを有するＩＣカードと、このＩＣカードにインストールされているアプリケーションの処理を指示する処理装置とからなるものにおいて、上記ＩＣカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置から指示された所定のアプリケーション記録領域に記録されているアプリケーションの処理を実行する際、または所定のアプリケーションをスロット内にインストールする際に、他のスロットへアクセスするアプリケーションであるか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段によりアプリケーションのインストールまたは実行を不許可とする手段とからなる。

【００１６】この発明のＩＣカードは、アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するものにおいて、上記ＩＣカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションのスロットを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなる。

【００１７】この発明のＩＣカードは、アプリケーションがインストールされている不揮発性メモリを有し、処理装置からの指示によりインストールされているアプリケーションを実行するものにおいて、上記ＩＣカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなる。

【００１８】この発明のＩＣカードは、アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するものにおいて、上記ＩＣカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、スロットを超過してアプリケーションが書込まれることを不許可とする手段を有する。

【００１９】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態について説明する。

【００２０】図１は、この発明のＩＣカード発行システムの概略構成を示している。

【００２１】このＩＣカード発行システムは、端末装置１１とＩＣカード１２とにより構成される。端末装置１１は、演算および人間からの入力を司る演算装置１１１と、ＩＣカード１２との入出力を司るリーダライタ１１２が結線１１３により接続されている。

【００２２】演算装置１１１は、演算を行うためのプロセッサを持ち、また人間系を含む外部よりの入力手段を持っている。ＩＣカード１２への要求と、結果ステータスの処理をここで行う。

【００２３】リーダライタ１１２は、演算装置１１１より要求を受け、その要求をカード挿入口１２０に挿入されているＩＣカード１２へと発行する。同様にＩＣカード１２からのステータスを受け取り、その結果を演算装置１１１へと報告する。

【００２４】また、ＩＣカード処理システムも、上記ＩＣカード発行システムと同じ構成となっている。

【００２５】ＩＣカード１２は、図１、図２に示すように、外部との接点となるコンタクト２０、および演算、制御を行うプロセッサ２１、一時データを配置するための揮発性メモリ（ＲＡＭ）２２、永続的にデータを保存するための不揮発性メモリ（ＥＥＰＲＯＭ）２３を持つ。またコンタクト２０を通じてリーダライタ１１２と通信を行う。上記不揮発性メモリ２３としては、フラッシュメモリ、ＦＲＡＭ等を用いても良い。

【００２６】プロセッサ２１は、端末装置１１からロードされるアプリケーションをＩＣカード１２用のカードアプレットＣＡＰに変換する機能を有している。

【００２７】上記プロセッサ２１の制御のもと、２種類のメモリ、揮発性メモリ２２と不揮発性メモリ２３が管理される。また、特に負荷の生じる演算を行うためのコプロセッサ２４を持つこともあり、これはプロセッサ２１の指示のもと演算を行う。

【００２８】データは、図１におけるコンタクト２０より入力され、一般に揮発性メモリ２２内に格納される。ここで受信されたデータは、プロセッサ２１により解析され、処理される。ここで、保存が必要なデータはプロセッサ２１の指示のもと不揮発性メモリ２３に書き込まれ、特殊な演算が可能なものはコプロセッサ２４へと処理の指示が送られる。また、ＲＡＭ２２では格納しきれない大きなデータなどが一時的に、ＥＥＰＲＯＭ２３の別領域に書き込まれることがある。

【００２９】上記ＥＥＰＲＯＭ２３は、図３、図４に示すように、カードＩＤ等が記録されるシステムデータ領域３１、領域チェック用のＢＣＣ領域３２、コミットバッファ領域としてのＣＢ領域３３、スロットを管理するスロット管理テーブル３４ａやアプリケーション間の許可状態を示す共有テーブル３４ｂが記録されるカードデータ領域３４等のシステム領域と、複数スロットからなり各スロットごとにアプリケーションが記録できるユーザアプリケーション領域３５とにより構成されている。ＢＣＣ領域３２は、カードデータ領域３４、ユーザアプリケーション領域３５の正しさをチェックするための領域である。

【００３０】ユーザアプリケーション領域３５は、たとえば、図４に示すように、＃０～＃７の８つのスロットにより構成されており、各スロット単位で、ユーザアプリケーションが記録されるようになっている。

【００３１】上記カードデータ領域３４に記録されるスロット管理テーブル３４ａは、図５に示すように、各スロットごとに、スロットに記録されるアプリケーションの状態ＳＴＳ、スロットに記録されるアプリケーション名（番号）ＡＩＤ、スロットのユーザアプリケーション領域３５における先頭位置（アドレス）ＴＯＰ、スロットのユーザアプリケーション領域３５におけるサイズＳＩＺＥにより構成されている。

【００３２】各スロットごとの先頭位置（アドレス）ＴＯＰ、サイズＳＩＺＥは、カード発行者をカード発行機（ＩＣカード発行システム）にて認定した際に、設定できるものである。

【００３３】アプリケーションの状態ＳＴＳとしては、アプリケーションの申請に基づくスロットの領域の設定時にＩＣカード発行システムで「Ｃ」が記録され、ＩＣカード処理システムでのアプリケーションのインストール時の準備段階時に「Ｐ」（Ｐｒｅｐａｒｅｄ）が記録され、ＩＣカード処理システムでのＩＣカードへのアプリケーションのインストール終了時に「Ｒ」（Ｒｅｇｉｓｔｅｒｅｄ）が記録されるようになっている。

【００３４】上記カードデータ領域３４に記録される共有テーブル３４ｂは、図６に示すように、各アプリケーションのモジュールに対する参照を許可するアプリケーションが記録されるようになっており、許可を行うアプリケーション名ＡＩＤのモジュール名と許可されるアプリケーション名ＡＩＤによって構成されている。

【００３５】上記ＩＣカード発行システムにおいて、ＩＣカード１２を発行する際の処理について説明する。

【００３６】すなわち、端末装置１１において発行者を特定している状態において、カードの発行やカードＩＤやスロットサイズ等が指示されているとともに、未記録状態のＩＣカード１２がリーダライタ１１２のカード挿入口１２０に挿入されている。上記スロットサイズは、アプリケーションのインストール者からの申請に基づいて設定されるようになっている。

【００３７】これにより、端末装置１１により設定されたカードＩＤがＥＥＰＲＯＭ２３のシステム領域３１に記録され、端末装置１１により設定されたスロットサイズに基づいてＥＥＰＲＯＭ２３のカードデータ領域３４のスロット管理テーブル３４ａに各スロットごとのユーザアプリケーション領域３５における先頭位置（アドレス）ＴＯＰとユーザアプリケーション領域３５におけるサイズＳＩＺＥとが記録され、対応するアプリケーションの状態ＳＴＳに申請を示す「Ｃ」が記録される。

【００３８】上述したスロットの管理は発行者により行われるようになっている。

【００３９】上記ＩＣカード処理システムにおいて、ＩＣカード１２にアプリケーションをインストールする際の処理について説明する。

【００４０】すなわち、端末装置１１においてアプリケーションのインストール者を特定している状態において、アプリケーションのインストールやアプリケーション名ＡＩＤや各アプリケーションのモジュールに対する許可アプリケーション等が指示されているとともに、上記ＩＣカード発行システムで発行されたＩＣカード１２がリーダライタ１１２のカード挿入口１２０に挿入されている。

【００４１】これにより、端末装置１１により設定されたアプリケーション名ＡＩＤがＥＥＰＲＯＭ２３のカードデータ領域３４のスロット管理テーブル３４ａに現在申請されている状態のスロットに対応して記録され、対応するアプリケーションの状態ＳＴＳに準備を示す「Ｐ」が記録される。

【００４２】この状態において、端末装置１１からＩＣカード１２アプリケーションがロードされることにより、ＩＣカード１２内のＥＥＰＲＯＭ２３のユーザアプリケーション領域３５にインストールされ、記録される。

【００４３】この際、スロット管理テーブル３４ａの準備中状態のスロットに対応して記録されているユーザア

プリケーション領域３５における先頭位置（アドレス）ＴＯＰに基づいて、アプリケーションが記録される。また、アプリケーションのサイズは、スロット管理テーブル３４ａの準備中状態のスロットに対応して記録されているアプリケーション領域３５におけるサイズＳＩＺＥに基づいて規定されている。

【００４４】したがって、アプリケーション領域３５におけるサイズＳＩＺＥを超過してスロット外にアプリケーションを書込もうとしたことが検出された場合は書き込みは不許可とされる。

【００４５】上記アプリケーションがインストールされた後、スロット管理テーブル３４ａの対応するスロットのアプリケーションの状態ＳＴＳに記録を示す「Ｒ」が記録される。

【００４６】たとえば、上述したアプリケーションの設定により、図７に示すように、スロット＃０に対してアプリケーション１が記録され、スロット＃１に対してアプリケーション２が記録され、スロット＃２に対してアプリケーション３が記録され、アプリケーション１がモジュール５１１～５１４からなり、アプリケーション２がモジュール５２１～５２４からなり、アプリケーション３がモジュール５３１～５３３からなる。

【００４７】この状態において、所定のアプリケーションのモジュールに対する許可アプリケーションの指示に基づいて、カードデータ領域３４の共有テーブル３４ｂに、所定アプリケーションのモジュールに対する参照を許可するアプリケーションが記録される。

【００４８】たとえば、図６に示すように、共有テーブル３４ｂにアプリケーション１のモジュール５１４に対してアプリケーション２が記録され、図７に示すように、アプリケーション１のモジュール５１４に対してアプリケーション２（モジュール５２２）による利用が許可されるようになっている。

【００４９】次に、各アプリケーション実行時のモジュールごとの領域確認処理（領域管理）について、図８に示すフローチャートを参照しつつ説明する。

【００５０】すなわち、プロセッサ２１は、所定のモジュールにおいて、他のモジュールの呼出しが行われた際に（ＳＴ１）、スロット管理テーブル３４ａを参照して現在のモジュールが属する領域（スロット）をその物理アドレスから確認するとともに、呼び出す他のモジュールが属する領域（スロット）をその物理アドレスから確認する（ＳＴ２）。この確認の結果、プロセッサ２１は、それらが同一領域（スロット）か否かを判断し（ＳＴ３）、この判断の結果が同一領域の場合、プロセッサ２１は、処理を継続する（ＳＴ４）。

【００５１】上記ステップ３の判断の結果、同一領域（スロット）できない場合、プロセッサ２１は、共有テーブル３４ｂを参照して呼び出す他のモジュールに対する参照を許可するアプリケーションを確認することにより（ＳＴ５）、現在のモジュールが呼び出す他のモジュールを参照できるか否かを判断（権限判断）する（ＳＴ６）。この判断の結果、呼び出す他のモジュールにおいて参照を許可している場合、プロセッサ２１は、処理を継続する（ＳＴ４）。

【００５２】上記ステップ６の判断の結果、呼び出す他のモジュールが参照を許可していない場合、プロセッサ２１は、処理の継続を否認し（アプリケーションの記録の不許可）、処理を終了する（ＳＴ７）。

【００５３】これにより、アプリケーションの跨りを領域跨りとして検出できる。また現在のモジュールと呼び出す他のモジュールのそれぞれが配置されている物理情報により判別が行えるので、データ偽造、データ破壊等を考慮しても、より高いセキュリテイが確保できる。また、従来システムのように対応表などを利用することなく、直接物理情報から決定できるのでより高速に処理が可能である。

【００５４】上記領域確認処理を、所定のアプリケーションを用いて処理を実行している際に行っているが、アプリケーションのインストール時に行ってインストールを不許可として良い。

【００５５】上記したように、スロットは明示的に領域管理と関係づけられ、インストールされるアプリケーションが使用できる最大領域として定義づけられる。このシステムでは、アプリケーションを入れるための器として定義されることになる。このため、各アプリケーション間の境界が明らかになり、例えばソフトウェアのモジュール５１４と５２２の間にアプリケーション１、２に跨る参照があっても、これはスロットを跨っていることにより検出が容易となる。

【００５６】逆に、アプリケーションごとにスロットとして領域の大きさを事前に規定することは、従来システムに比べ、アプリケーション領域の自由な拡張が難しい、ということが挙げられるが、使用可能な全体領域が限られるＩＣカードにおいては、一般にアプリケーションの基本設計時にほぼその使用領域が決定され、その後自由に拡張されるようなことはない。これは、領域の上限が低いため、動的に領域獲得を行うと容易に領域不足を引き起こしてしまうからである。

【００５７】また、物理領域としてスロットを分ける更なる理由の一つとして、一つのアプリケーションが修復不能な状態になったとしても、その領域そのものを切り離すことにより、他スロットにあるアプリケーションへの影響は及ばないように実現できる。

【００５８】したがって、発行後にアプリケーションのインストールが可能なＩＣカードと、ＩＣカードへの入出力手段となる端末装置を具備するＩＣカードシステムにおいて、各アプリケーションが事前に確定されたスロット内でのみ領域を拡張しうるようにスロット領域を確定することができる。

【００５９】また、アプリケーションが使用する領域をそのまま制限された物理領域にマッピングすることにより、領域管理をセキュリテイ管理と連動させ、アプリケーションの独立性を領域監視により確保することができる。

【００６０】この構成においては、領域をそのアプリケーションと対応づけることにより、各アプリケーションの独立性を領域単位で保証することを可能とし、高いセキュリティ性をも実現することができる。

【００６１】すなわち、ＩＣカードにおいて発行後に載せられる複数アプリケーションを明示的に領域を分割し、管理することにより、他のアプリケーションの好ましくない影響を排除し、アプリケーションごとの柔軟な管理を効率よく実現することができる。

【００６２】

【発明の効果】以上詳述したように、この発明によれば、ＩＣカードの発行後に、このＩＣカードに対するアプリケーションのインストールが行えるものにおいて、上記ＩＣカードが不揮発性メモリを有し、上記ＩＣカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域としてのスロット内でのみ領域を拡張しうるようにスロット領域を確定することができるＩＣカード発行システムとＩＣカード処理システムとＩＣカードを提供できる。

【図面の簡単な説明】

【図１】この発明の実施形態のＩＣカード発行システムの概略構成を示す図。

【図２】ＩＣカードの概略構成を示すブロック図。

【図３】ＥＥＰＲＯＭの概略構成を示す図。

【図４】ＥＥＰＲＯＭのユーザアプリケーション領域の概略構成を示す図。

【図５】スロット管理テーブルの構成例を説明するための図。

【図６】共有テーブルの構成例を説明するための図。

【図７】各スロットとアプリケーションの関係を説明するための図。

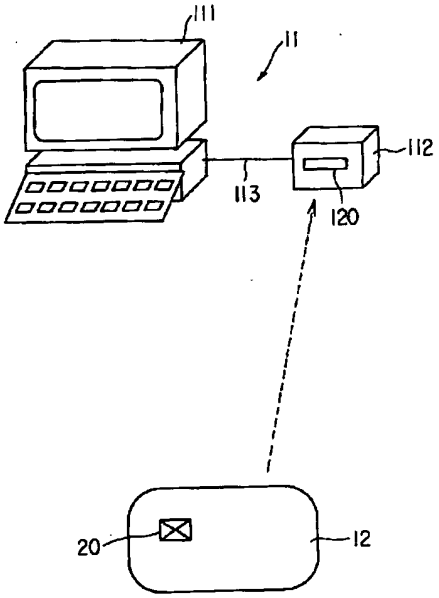
【図８】各アプリケーションのモジュールごとの領域確認処理を説明するためのフローチャート。

【図９】従来の各スロットとアプリケーションの関係を説明するための図。

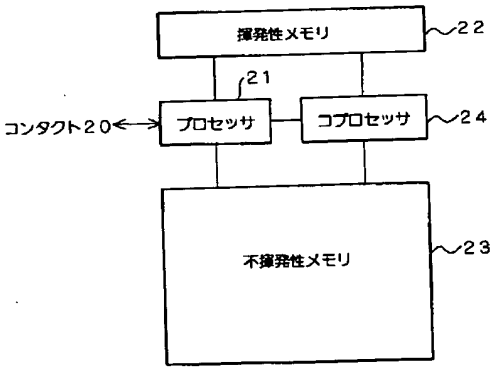
【符号の説明】

１１…端末装置
１２…ＩＣカード
２１…プロセッサ
２２…揮発性メモリ（ＲＡＭ）
２３…不揮発性メモリ（ＥＥＰＲＯＭ）
１１２…リーダライタ

【図１】



【図２】

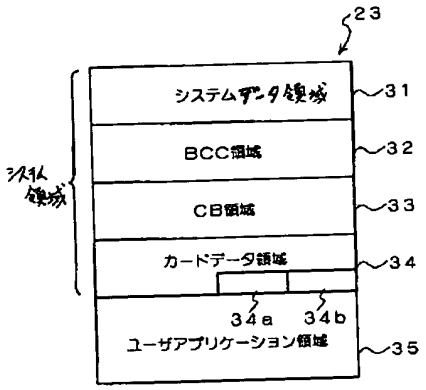


【図６】

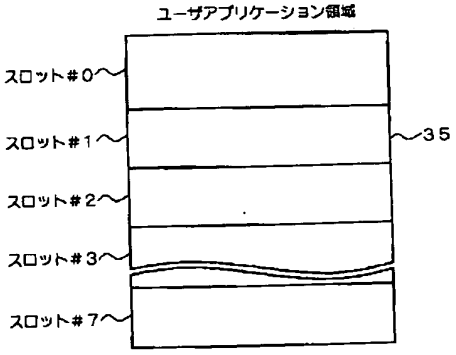
現在処理中のアプリケーション名	現在処理中のモジュール名	許可されるアプリケーション名
AP1	514	AP2

34b

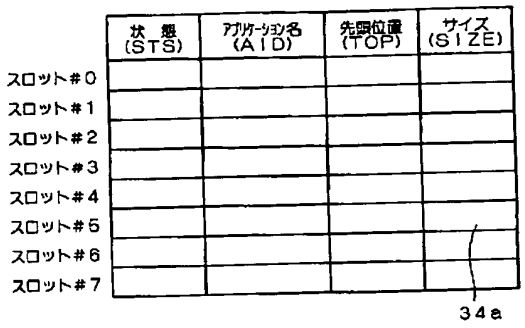
【図３】


23
システムデータ領域
31
BCC領域
32
CB領域
33
カードデータ領域
34
34a
34b
ユーザアプリケーション領域
35
システム領域

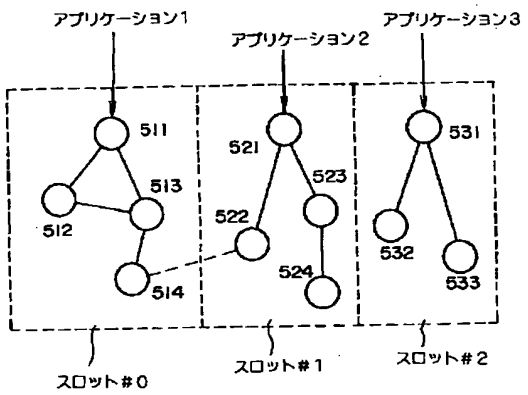
【図４】


ユーザアプリケーション領域
スロット#0
スロット#1
スロット#2
スロット#3
スロット#7
35

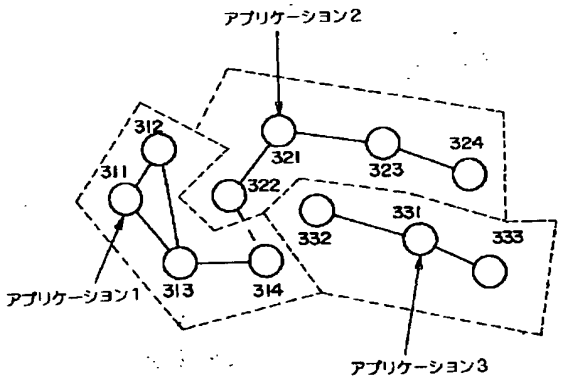
【図５】


状態 (STS)
アプリケーション名 (AID)
先頭位置 (TOP)
サイズ (SIZE)
スロット#0
スロット#1
スロット#2
スロット#3
スロット#4
スロット#5
スロット#6
スロット#7
34a

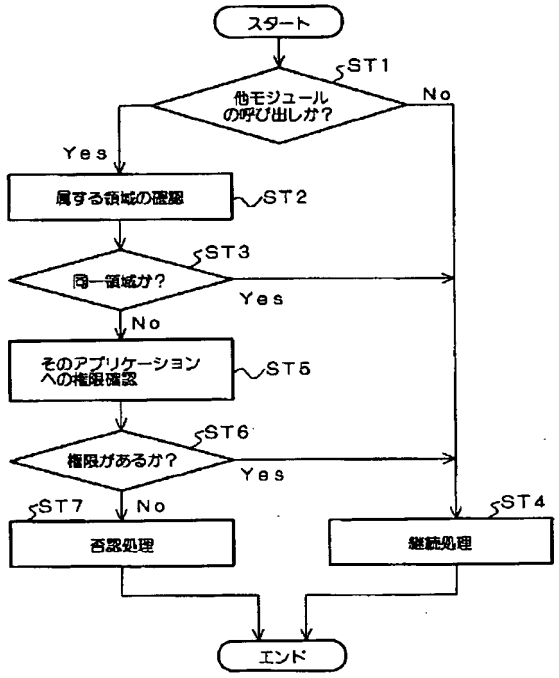
【図７】


アプリケーション1
アプリケーション2
アプリケーション3
511
512
513
514
521
522
523
524
531
532
533
スロット#0
スロット#1
スロット#2

【図９】


アプリケーション2
311
312
313
314
321
322
323
324
331
332
333
アプリケーション1
アプリケーション3

【図８】


スタート
ST1
他モジュールの呼び出しか？
No
Yes
属する領域の確認
ST2
ST3
同一領域か？
Yes
No
そのアプリケーションへの権限確認
ST5
ST6
権限があるか？
Yes
ST7
No
否認処理
ST4
継続処理
エンド